Quest ActiveRoles Server

Product Overview

Version 5.2

QUEST SOFTWARE

Warranty

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

Trademarks

Quest® ActiveRoles Server is a trademark of Quest Software, Inc. Other trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
8001 Irvine Center Drive
Irvine, CA 92618
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Quest ActiveRoles Server
Updated – February 14, 2005
Software version – 5.2

Contents

About Quest Windows Management

Quest Software, Microsoft's 2004 Global Independent Software Vendor Partner of the Year, provides solutions that simplify, automate and secure Active Directory, Exchange and Windows environments. The Quest Windows Management group delivers comprehensive capabilities for secure Windows management and migration. For more information on Quest Software's Windows Management group, please visit www.quest.com/microsoft.

About Quest Software, Inc.

Quest Software, Inc. provides software to simplify IT management for 18,000 customers worldwide, including 75 percent of the Fortune 500. Quest products for application, database and Windows management help customers develop, deploy, manage, and maintain the IT enterprise without expensive downtime or business interruption. Headquartered in Irvine, Calif., Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone	949.754.8000 (United States and Canada)
Email	info@quest.com
Mail	Quest Software, Inc. 8001 Irvine Center Drive Irvine, CA 92618 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Customer Support

Quest Software's world-class support team is dedicated to ensuring successful product installation and use for all Quest Software solutions.

SupportLink	www.quest.com/support
Email at	support@quest.com.

You can use SupportLink to do the following:

- Create, update, or view support requests
- Search the knowledge base
- Access FAQs
- Download patches

Introduction

Quest ActiveRoles Server automates user provisioning in Active Directory, Exchange, and Windows. With role-based security, HR and ERP system integration, automated group management, easy-to-use Web interfaces, and a comprehensive software development kit (SDK) for fast implementation of custom components, ActiveRoles Server provides a practical approach to complete user lifecycle management for the Windows enterprise.

ActiveRoles Server enables an organization to develop a flexible administration framework that suits their needs, while ensuring secure delegation of tasks, reduced workload, and lower costs. It also enables the integration of diverse corporate data sources and provisioning processes, which can expedite business workflow and eliminate data inconsistencies.

This document is designed for IT managers, network administrators, operations managers, and security managers who are evaluating ActiveRoles Server and want to learn how it works. The document examines:

- Features and benefits of ActiveRoles Server
- The system's components and architecture
- Access Templates, Policy Objects, and Managed Units
- Support for Group Policy management
- Support for Active Directory security management
- Customization with the ActiveRoles Server ADSI Provider and support for scripting
- Rule-based management of group membership lists
- Capabilities of the ActiveRoles Server Web Interface
- System Requirements
- Licensing
- Example scenarios in which ActiveRoles Server might be used

Features and Benefits

The key features and benefits of ActiveRoles Server include the following.

Secure Architecture

ActiveRoles Server creates a secure layer between administrators and managed data sources, which ensures consistent policy enforcement, facilitates auditing, and eliminates the need for individual accounts and passwords that could be used for unauthorized purposes.

Unified Management Console

ActiveRoles Server enables you to perform all tasks related to Active Directory administration from a single MMC- or Web-based interface. You can define "Rules & Roles," administer users and computers, manage Group Policy, track changes, and manage native permissions in Active Directory from a single management console.

Reliable Enforcement of Corporate Rules

ActiveRoles Server allows you to enforce corporate rules and constraints for a wide range of conditions, having directory updates invoke procedures that police what is put in the directory, what else must be changed, who must approve and other administrator-defined conditions. It eliminates reliance on client-side processing for highly secure and highly reliable directory administration.

Role-Based Administrative Structure

ActiveRoles Server facilitates the creation of a role-based administrative structure, covering both the granularity and scope of delegation, to ensure consistency across your organization and speed administrative privilege delegation. You can delegate administrative control of users, groups, computers and other Active Directory objects, as well as Group Policy objects, and use customizable permission templates to simplify the process of defining administrative roles.

Flexible Administrative Views

ActiveRoles Server offers rule-based administrative views (Managed Units) to separate the administrative framework from the Active Directory design by overlaying OU, domain and forest boundaries. Managed Units assist in the administration of interdependent hierarchical directory structures and multiple forests.

Group Policy Management

ActiveRoles Server increases Group Policy administrator productivity and ensures the correct workflow by integrating role-based access control, corporate rule enforcement and system interfaces for managing Group Policy. You can view the resultant set of policies (RSoP) for any user or computer, and perform "what-if" analyses to evaluate the effect of proposed changes. You can quickly find all Group Policy objects that include specified settings or properties.

Automated Account Provisioning

ActiveRoles Server makes it possible to automate provisioning tasks and integrate information from other databases, extending administrative workflow automation to other data sources such as HR and ERP systems, increasing productivity, and eliminating costly errors.

User Management Auditing and Advanced Reporting

ActiveRoles Server provides a complete audit trail, showing who performed what actions and who tried to perform actions that were not permitted. A rich suite of reports assists in change tracking and policy enforcement audits, and Active Directory monitoring and analysis.

Support for Active Directory Service Interfaces

Industry-standard interfaces enable custom scripts and applications to communicate with Active Directory through ActiveRoles Server, taking full advantage of this product's security, workflow integration and reporting benefits.

Dynamic Group Membership

ActiveRoles Server includes the facility to automatically keep group membership lists up to date, eliminating the need to add and remove members manually. Rule-based management of membership lists reduces the cost of maintaining groups. In addition, it increases the accuracy and reliability of message distribution through membership in distribution groups, and increases the consistency of security settings through membership in security groups.

Virtual Attributes

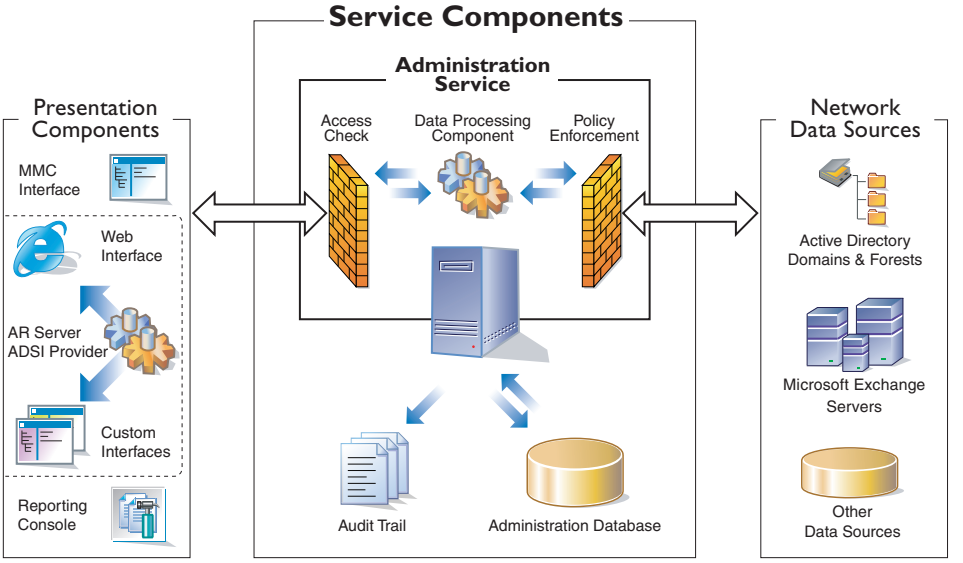
Virtual attributes provide alternative storage for object properties that do not exist in the default Active Directory schema. You can define virtual attributes using data that resides in other sources or repositories. This allows you to create additional object properties without extending the Active Directory schema. Properties that are stored as virtual attributes are displayed in the UI, and can be administered in the same way as those stored in Active Directory.

MMC and Web Interfaces

The ActiveRoles Server MMC interface facilitates directory administration and lowers the learning curve required to administer Active Directory and Exchange 2000/2003. An advanced "three-pane" interface enhances productivity for even the most sophisticated IT professional. Web interfaces are also available for administrators, help desk personnel and users for self-administration. These Web interfaces can be easily customized to meet your particular needs and corporate environment.

Technical Overview

ActiveRoles Server divides the workload of directory administration and provisioning into three functional layers—presentation components, service components, and network data sources.



The presentation components include client interfaces for the Windows platform and the Web, which allow regular users to perform a precisely defined set of administrative activities. Reporting Console facilitates automated generation of reports on management activities.

The service components constitute a secure layer between administrators and managed data sources. This layer ensures consistent policy enforcement, provides advanced automation capabilities, and enables the integration of business processes for administration of Active Directory, Microsoft Exchange, and other corporate data sources.

The Administration Database stores information about all permission and policy settings, and other metadata related to the ActiveRoles Server configuration.

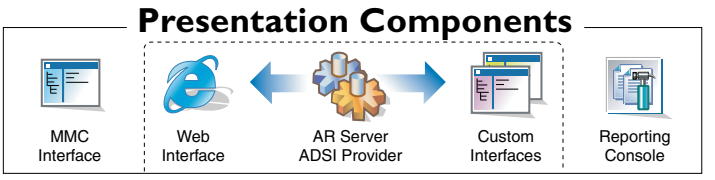
On a very high level, the ActiveRoles Server components work together as follows to manipulate directory data:

1. An administrator uses the MMC interface or Web interface to access ActiveRoles Server.
2. The administrator submits an operation request, such as a query or data change to the Administration Service.
3. On receipt of the operation request, the Administration Service checks whether the administrator has sufficient permissions to perform the requested operation (access check).
4. The Administration Service ensures that the requested operation does not violate the corporate policies (policy enforcement).
5. The Administration Service performs all actions required by the corporate policies, before committing the request (policy enforcement).
6. The Administration Service issues operating system function calls to perform the requested operation on network data sources.
7. The Administration Service performs all related actions required by the corporate policies, after the request is processed by the operating system (policy enforcement).
8. The Administration Service generates an audit trail that includes records about all operations performed or attempted with ActiveRoles Server. Directory-change tracking reports are based on the audit trail.

Let us examine the three component layers.

Presentation Components

The presentation components include user interfaces to serve a variety of needs. The user interfaces accept commands, display communication, and give results in a clear, concise fashion:



MMC Interface

The MMC Interface is a comprehensive administrative tool for managing Active Directory and Microsoft Exchange. It enables you to specify administrative roles and delegate control, define administrative policies and automation scripts, easily find directory objects, and perform administrative tasks.

Web Interface

Via the Web interface, intranet users with sufficient administrative rights can connect to ActiveRoles Server to perform basic administrative tasks, such as modifying user data or adding users to groups. The Web interface provides departmental and help-desk personnel with the administrative capabilities they need.

Custom Interfaces

In addition to the MMC and Web interfaces, ActiveRoles Server enables the development of custom interfaces that use the ActiveRoles Server ADSI Provider to access the features of ActiveRoles Server. Administrators familiar with scripting and programming can create custom interfaces to meet specific needs of the network administration.

ActiveRoles Server ADSI Provider

The ActiveRoles Server ADSI Provider operates as part of Presentation Components to enable custom user interfaces and applications to access Active Directory services through ActiveRoles Server. The ActiveRoles Server ADSI Provider translates clients' requests into DCOM calls and interacts with the Administration Service.

The ActiveRoles Server ADSI Provider allows custom scripts and applications, such as Web-based applications, to communicate with Active Directory, while taking full advantage of the security, workflow integration and reporting benefits of ActiveRoles Server. For example, using the ActitveRoles Server ADSI Provider, Web-based pages can be created such that user property modifications made by help-desk operators are restricted by the corporate rules enforced by ActiveRoles Server.

ActiveRoles Server Collector and Reporting Console

ActiveRoles Server offers comprehensive reporting to monitor administrative actions and the state of directory objects. Reporting components include the ActiveRoles Server Collector, and Reporting Console.

The ActiveRoles Server Collector is used to gather data required for reporting. The Collector retrieves data from the following sources, accessing the data sources through the Administration Service:

- Active Directory
- Administration Database
- ActiveRoles Server Log

The Reporting Console displays and customizes reports, based on the data gathered by the Collector. Report jobs can be configured to run automatically in unattended mode. ActiveRoles Server comes with an extensive suite of customizable reports that cover all administrative actions available in the product.

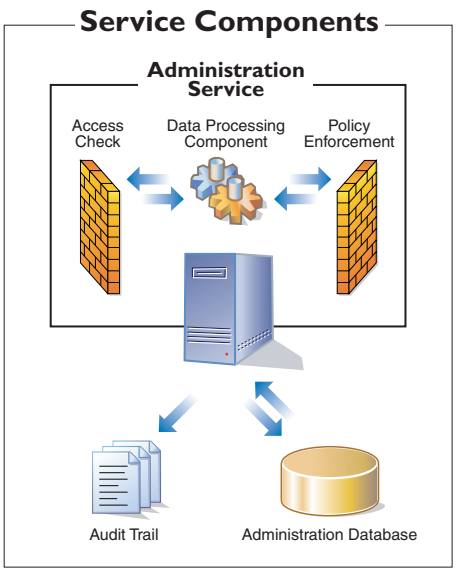
Data from the ActiveRoles Server Log is used to produce reports for change tracking audits. These reports indicate the actions performed, the success or failure of each action, and the attribute changes by ActiveRoles Server.

Data from the Administration Database is used to create reports to monitor the level of access each user has to objects within ActiveRoles Server. In addition, the data can be used to learn which corporate rules are enforced by ActiveRoles Server.

Data from Active Directory is used to produce reports that can be used for Active Directory monitoring and analysis. Such reports provide information about the state of user accounts, groups, and other objects in Active Directory.

Service Components

At the heart of ActiveRoles Server lies the Administration Service—a powerful, rules-based proxy for the management of network data sources. The Administration Service features advanced delegation capabilities and provides the ability to enforce administrative policies that keep data current and accurate. The Administration Service acts as a bridge between the presentation components and network data sources. In large networks, multiple Administration Services can be deployed to improve performance and ensure fault tolerance.



Data Processing Component

The data processing component accepts administrative requests and validates them by checking permissions and rules stored in the Administration Database. The component manages the network data sources, retrieving or changing the appropriate network object data based on administrative requests and policy definitions.

The data processing component operates as a secure service. It employs special user accounts with sufficient privileges to log on to the domains registered with ActiveRoles Server (managed domains). The access to the managed domains is limited by the access rights of those user accounts.

For security reasons, it may be unacceptable for the data processing service account to possess administrative access to an entire managed domain. To address this issue, ActiveRoles Server supports the use of non-administrator accounts for the Administration Service logon. When this service logs on with a non-administrator account, ActiveRoles Server retains its entire functionality, but prevents users from performing actions that are not permitted on that service account.

For an organization to which administration of only part of a domain is outsourced, the ability to use a non-administrator account provides all benefits of ActiveRoles Server without needing administrative access to the entire domain, access that such organizations normally do not have.

Administration Database

The Administration Service uses the Administration Database to store configuration data. The configuration data includes definitions of objects specific to ActiveRoles Server, assignments of administrative roles and policies, and procedures used to enforce policies.

The Administration Database is only used to store ActiveRoles Server configuration data. It does not store copies of the objects that reside in the managed data sources, nor is it used as an object data cache.

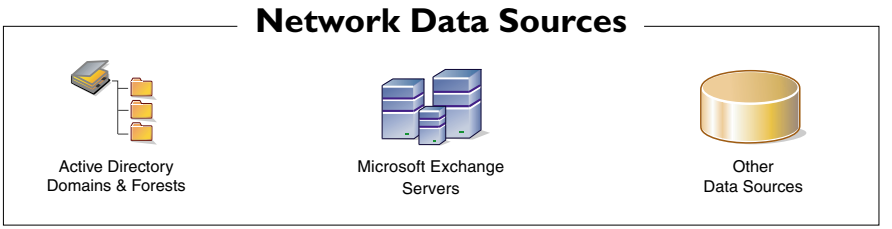
ActiveRoles Server employs the Microsoft SQL Server to maintain the Administration Database. The replication capabilities of SQL Server facilitate the implementation of multiple equivalent Administration Databases used by different Administration Services.

Audit Trail

The data processing component provides a complete audit trail by creating records in the event log on the computer running the Administration Service. The log shows all actions performed and by whom, including actions that were not permitted. The log entries display the success or failure of each action, as well as which attributes were changed.

Network Data Sources

Through the Administration Service, ActiveRoles Server accesses and controls the object data stored in the following data sources:



- **Active Directory Domains & Forests**—Provide the directory object information in Active Directory domains.
- **Microsoft Exchange Servers**—Provide information about mailboxes maintained by Microsoft Exchange.

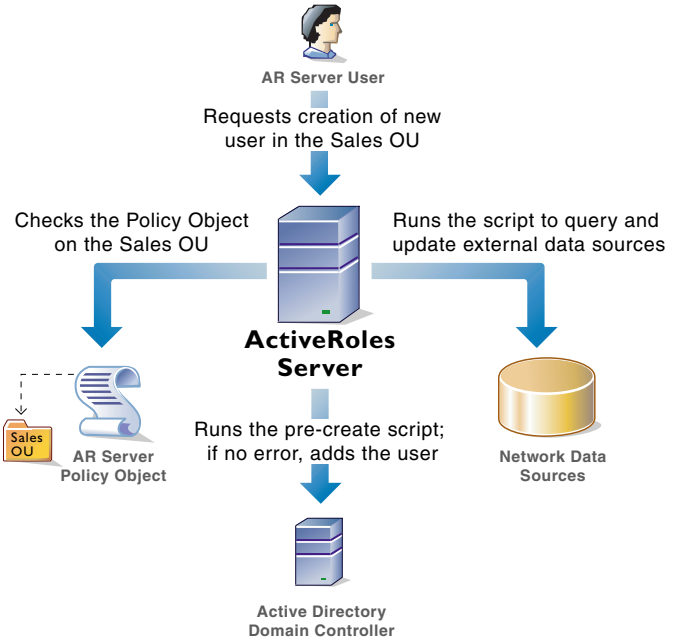
- **Other Data Sources**—Provide information about objects that exist outside of Active Directory. This includes information from corporate databases, such as human resources databases, and information about computer resources, such as services, printers, and network shares.

ActiveRoles Server is designed to help with the use and management of these data sources. Directory administrators can define and enforce business rules and policies to ensure that the data in the managed data sources remains current and accurate.

With ActiveRoles Server, you can utilize the information stores from a wide variety of data sources in your network, such as human resource data or inventories. You can use custom scripts to integrate these important data sources. This reduces the duplication of work, reduces data pollution, and allows for the validation of information that is often stored in more than one database.

ActiveRoles Server makes it possible for a custom script to receive control upon a request to perform an administrative operation, such as object creation, modification, or deletion. Custom scripts are invoked through Policy Objects, which ActiveRoles Server uses to enforce corporate rules (see "Policy Objects to Enforce Corporate Rules" later in this document).

For example, you could implement a Policy Object containing a custom script that will receive control whenever ActiveRoles Server is requested to create a user object in a certain OU:



The Policy Object may be configured so that ActiveRoles Server continues with the user creation only after a certain piece of the script (the pre-create event handler) has successfully executed. In this way, the script prohibits the creation of user objects whose properties violate corporate rules. It prevents the population of object properties with values taken from external data sources, and generates default property values in accordance with the corporate rules.

The Policy Object may also be configured to pass control to another piece of the script (the post-create event handler) immediately after a user object is successfully created. This enables the script to trigger additional actions, required by corporate rules, after the object has been created. For example, it can update external data stores, provision the user with access to resources, and notify that the user object has been created.

For additional information, see the section “ADSI Provider and Script Policy to Support Customization” later in this document.

Security and Administration Elements

ActiveRoles Server offers three key security and administration elements, which are stored as objects in the Administration Database:

- Access Templates
- Policy Objects
- Managed Units

These elements enable any user or group in Active Directory to be given limited and effectively controlled administrative privileges.

Users and groups that are given administrative permissions in ActiveRoles Server are referred to as *Trustees*. Trustees can be assigned to Managed Units or directory objects and containers.

Trustees do not need special administrative rights within Active Directory. To give Trustees access to Active Directory, ActiveRoles Server implements proxy mechanisms that use Access Templates to specify the level of access. When Trustees exercise their access permissions, these mechanisms use Policy Objects to trigger additional actions, such as running integration scripts and validating input data.

When designating a user or group as a Trustee, you must specify the Access Templates that control what the Trustee can do. Permissions granted to a group are extended to all members of that group. To reduce administration time, administrative control should be delegated to groups, rather than to individual users.

To implement policy constraints and automation, you must configure and apply Policy Objects that invoke built-in or custom procedures upon administrative requests. Policy procedures may include running custom scripts to synchronize Active Directory data with other data sources, performing a data validity checkup, and initiating additional administrative operations.

Access Templates for Role-based Administration

An *Access Template* is a collection of permissions that define what actions can be performed by an administrative role. ActiveRoles Server applies Access Templates to directory objects, containers, and administrative views (Managed Units) in relation to groups and users designated as Trustees.

ActiveRoles Server offers an extensive suite of preconfigured Access Templates that represent typical administrative roles, enabling the correct level of administrative authority to be delegated quickly and consistently. Access Templates significantly simplify the delegation and administration of management rights, speed up the deployment of the delegation model, and reduce management costs.

The preconfigured Access Templates provide access rights for the following areas:

AREA	DESCRIPTION
ACTIVE DIRECTORY	Management of Active Directory objects. Templates in this category facilitate granular delegation of management rights for: • Domain objects and organizational units • User, contact, group, and inetOrgPerson objects • Computer, printer, and shared folder objects Provided are templates that allow for a wide range of administrative tasks and templates that limit access to selected properties of Active Directory objects.

AREA	DESCRIPTION
EXCHANGE	Management of Microsoft Exchange 2000/2003 mail recipients. This category includes templates to delegate the following administrative tasks: • Manage all recipient settings • Use Exchange Tasks Wizard • Manage e-mail addresses • Configure general message settings • Configure advanced message settings Also provided are permission templates that specify access to selected Exchange related properties of users, groups, and contacts.
GROUP POLICY	Group Policy management and modeling. This category includes permission templates to delegate the following administrative tasks: • Manage Group Policy on selected domains and OUs • Manage GPO links on selected domains and OUs • Use Group Policy modeling for selected objects/containers • View and modify selected Group Policy objects • View and modify selected settings in Group Policy objects Templates in this category provide very fine permission granularity, such as the restriction of access to individual policy settings within Group Policy objects.

AREA	DESCRIPTION
COMPUTER RESOURCES	Management of computer local resources. Templates in this category facilitate granular delegation of management tasks for: • Local users and groups • Services • Network shares (shared directories) • Printers and print jobs In this category, there are templates for specific administrative roles, such as Printer Operator or Service Operator, and templates that specify access to selected properties of computer local resources.
EDM CONFIGURATION	Management of ActiveRoles Server proprietary objects and configuration settings. Templates in this category enable delegation of ActiveRoles Server configuration management. The following tasks can be delegated: • Administer Managed Units, Policy Objects, or Access Templates in selected containers • Configure replication (add or remove replication partners) • Add or remove managed domains In addition, there are templates that provide access to individual properties of Managed Units, Policy Objects and Access Templates.

It is also possible to create custom Access Templates based on business requirements.

Access Templates enable centralized administrators to define administrative roles with various levels of authority, speeding up the deployment of access control and streamlining change tracking of permission settings across the enterprise.

Access Templates can be modified at any time. When an Access Template is modified the permission settings for all objects based on that template change accordingly.

Permissions

Permissions represent authorization to perform operations on objects of a certain type (class), such as User, Group, or Computer. Unless permission to perform an operation is explicitly granted, it is denied. Permissions can also be explicitly denied.

Permissions can be specified at the object level or property level. Permissions allowed or denied at the object level apply to the entire object. Permissions allowed or denied at the property level apply only to specific properties. For example, on a container, you could set an object-level permission that allows a particular group to create child objects in that container. Another example would be setting property-level permissions that allow particular users to change the Home Address property of their user accounts.

There are two types of permissions: *explicit* and *inherited*.

Explicit Permissions

Explicit permissions are those that are defined directly on an object. Explicit permissions are defined by applying (linking) Access Templates directly to an object. For example, when an Access Template is linked to a user account, the permissions on the account are explicit permissions.

Inherited Permissions

Inherited permissions are those that are propagated to an object from a parent object or collection. Inherited permissions result from applying Access Templates to administrative views (Managed Units) and Active Directory containers (Organizational Units or entire domains). Inherited permissions affect all objects within a view or container down the directory tree. Defined for a parent object or collection, inherited permissions can only be modified by changing the parent's permission settings.

Permissions defined on a Managed Unit, or permissions inherited by a Managed Unit, are inherited by all its members. Because of this inheritance, when objects change their memberships in Managed Units, permission settings on those objects also change. This provides the ability to regulate permission settings by using Managed Units' membership rules.

Policy Objects to Enforce Corporate Rules

A *Policy Object* is a collection of administrative policy definitions that specify corporate rules to be enforced. Access Templates define who can make changes to a piece of data, and Policy Objects control what changes can be made to the data. ActiveRoles Server enforces corporate rules by linking Policy Objects to:

- Administrative views (Managed Units)
- Active Directory containers
- Individual (leaf) directory objects

Policy Objects define the behavior of the system when directory objects are created, modified, moved, or deleted. Policies are enforced regardless of a Trustee's permissions.

A Policy Object includes stored policy procedures and specifications of events that activate each procedure. Based on policy requirements, a policy procedure could:

- Validate specific property values
- Allow or deny entire operations
- Trigger additional actions

A Policy Object associates specific events with its policy procedures, which can be built-in procedures or custom scripts. This provides an easy way to implement sophisticated validation criteria, synchronize different data sources, and combine a number of administrative tasks into a single batch.

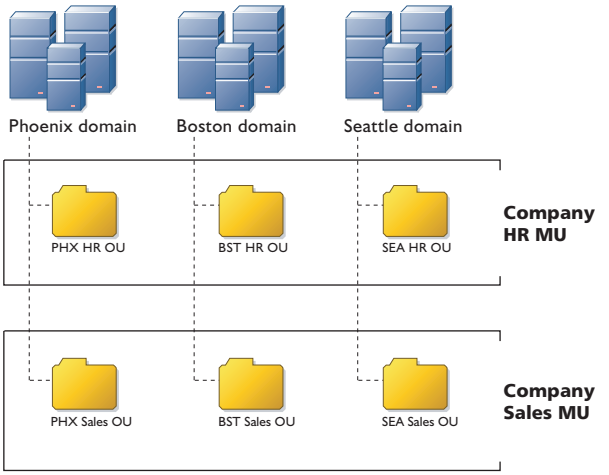
Policy Objects can be linked to Managed Units or individual containers. When linked to a Managed Unit or container, a Policy Object affects all member objects, including those located in the child containers. As an example, a Policy Object that specifies object naming conventions or other corporate standards can be linked to a directory container. If an administrator attempts to create a new object or modify an existing object in the container, the naming conventions or other corporate standards determine whether the changes are accepted or rejected. In addition, other corporate data sources could be requested and updated when a directory object is created or modified.

Policy Objects can also be linked to individual leaf objects, such as user objects. For example, a business rule could prohibit changes being made to group memberships when copying a certain user object.

Managed Units to Provide Administrative Views

A *Managed Unit* is a collection of objects collectively managed with ActiveRoles Server, created for the distribution of administrative responsibilities, enforcement of business rules and corporate standards, and management of complex network environments. Using Managed Units, the management framework can be separated from the Active Directory design. Directory objects can easily be grouped into administrative views, regardless of their location in Active Directory.

For example, the Active Directory design might be based on geographic location, with domains named after cities or regions and Organizational Units named after corporate departments or groups. However, Managed Units could be designed to manage specific departments or groups that are divided across multiple geographic locations.



In this example, each AD domain has a Human Resources (HR) OU and a Sales OU. The ActiveRoles Server design has an HR MU and a Sales MU. The HR MU enables administrators to configure the policies and security restrictions needed for all HR users in one location, while the Sales MU enables the same for all Sales users.

Managed Units are defined with the use of membership rules—criteria used by ActiveRoles Server to evaluate whether or not an object belongs to a given Managed Unit. This enables Managed Units to dynamically change as the network environment changes. For example, you can define a Managed Unit by specifying rules that include all objects whose properties match specific conditions. When the network environment changes, the specified rules will force the new or modified objects to be members of the correct Managed Unit.

Managed Units extend the functionality of organizational units (OUs), providing convenient scope to delegate administration and enforce corporate rules. A Managed Unit has the following characteristics:

- Represents a collection of objects (one object can belong to more than one Managed Unit)
- Supports rule-based specifications for its members (a Managed Unit only holds objects that satisfy the membership rules specified for the Managed Unit)
- Can hold directory objects that reside in different Organizational Units, domains, forests, and other Managed Units

ActiveRoles Server ensures that permission and policy settings specified for a Managed Unit are inherited by all objects that belong to that Managed Unit. When a directory container belongs to a Managed Unit, all child objects in that container inherit the permission and policy settings defined at the Managed Unit level. This inheritance continues down the directory tree within all container objects that are members of the Managed Unit.

Group Policy Management

ActiveRoles Server provides the ability to manage Group Policy—an important feature of Microsoft Windows Server that enables IT administrators to control user access to applications and network resources, and to establish uniform desktop configurations.

ActiveRoles Server allows the delegation of responsibilities to create, modify, and assign (link) Group Policy objects to Organizational Units and domains, and offers user interfaces for assistant administrators to perform these tasks. It also enables assistant administrators to delete and disable Group Policy objects and links, and to change the inheritance options for Group Policy objects and links.

Delegation of Group Policy administration can be controlled and made secure using corporate rules and roles. Corporate rules can be used to constrain administrators' operations on Group Policy, enforcing correct workflow. Role-based delegation enables Group Policy management to be limited by Organizational Unit (OU) or domain. This ensures that administrators do not change Group Policy for users and computers outside their scope of authority.

ActiveRoles Server allows a custom script to receive control upon a request to modify Group Policy. The script may perform verification steps, or trigger additional actions to handle the modification based on corporate rules, rather than on access permissions. For example, even if a user has sufficient permissions to modify Group Policy on a given OU, the modification of links to some Group Policy objects may still be denied by corporate rules, because it may have an unacceptable effect on the Group Policy infrastructure. Another example could be a constraint that prevents particular Group Policy objects being linked to certain OUs.

Group Policy Modeling

To simplify Group Policy implementation and troubleshooting, ActiveRoles Server offers Group Policy modeling—a feature that enables the administrator to determine how Group Policy settings are applied to users and computers. Group Policy modeling is useful when the administrator wants to:

- Simulate the effect of specific policy settings on a computer, user, domain, or Organizational Unit
- Simulate the effect of Group Policy on newly created users or computers, in a particular Organizational Unit

- Test the Group Policy effect in the following situations:
    - The user and the computer are in different security groups
    - The user and the computer are in different Organizational Units
    - The user or the computer is moving to a new location
- Create a slow network simulation
- Create a loop-back simulation

The Group Policy Modeling wizard provides the ability to simulate a Group Policy deployment to apply to users and computers, before actually applying the policies. Based on the input supplied by the administrator, the Group Policy Modeling wizard creates and saves a query, which represents the resultant policy settings of the combined Group Policy objects.

The display also shows which Group Policy object is responsible for each setting. The administrator can use the results of Group Policy modeling to construct a "What If" scenario, to predict the effect of changes made to policy settings. "What If" analysis enables the administrator to calculate the resultant set of policies before making any changes to Group Policy. This prevents implementation of a Group Policy without knowing exactly what the policies will affect.

Group Policy modeling helps administrators plan for growth and reorganization. When a change in Group Policy is necessary, the administrator can run a series of Group Policy modeling queries to simulate what will happen to a user if they are moved to another location, security group, or to another computer. The administrator can see what policy settings will be applied and which files will automatically be loaded after the change.

Group Policy Reporting

To increase Group Policy administration efficiency, ActiveRoles Server provides HTML reports for Group Policy objects and for Group Policy Modeling data. Group Policy reports are viewable via both the MMC Interface and Web Interface.

Reports for Group Policy objects allow you to quickly view all the settings contained in a Group Policy object. You can fully expand the report to view all settings, or expand and examine individual sections within the report. Each setting can be modified by clicking on it in the report. Summary information, such as the object's properties, links, delegation, security and WMI filtering, is also included.

Similar reports are provided for Group Policy Modeling data. For each Group Policy Modeling query, the report is split into two sections: **Summary** and **Settings**.

The **Summary** section includes the following information:

- Name of the user, computer, or container for which the Group Policy Modeling data was gathered.
- List of Group Policy objects that affect the selected user, computer or container, and the container to which each Group Policy object is linked.
- Simulated security group membership of the selected user or computer.

The **Settings** section provides a report of the final values of all policy settings that would be applied, and the Group Policy object that would determine each value (winning GPO). You may modify the corresponding setting in the winning GPO by clicking a policy setting in the report.

When a Group Policy report is created, it is possible to transfer the reported data to a file for printing or viewing. Using a context menu, you can save the report to a file in either HTML or XML format.

Role-Based Management of Group Policy

To facilitate delegated administration of Group Policy, ActiveRoles Server provides the following capabilities:

- Granular delegation of the management of Group Policy settings in Group Policy objects
- Read-only display of Group Policy settings whose modification by the delegated administrator is forbidden
- Ability to search for Group Policy objects based on Group Policy settings or GPO properties
- Centralized display of the GPO links that are applied to a given OU or domain, including the links inherited from parent containers

Granular permissions on Group Policy settings make it possible to delegate the precise set of permissions required for a Group Policy administrator to complete a given task, no more and no less. Although Active Directory provides for property-level access control, it only permits delegated administration of Group Policy settings on an all-or-nothing basis.

ActiveRoles Server comes with a suite of pre-configured Access Templates to delegate administration of Group Policy to users or groups (Trustees). Below are some examples of such Access Templates:

TEMPLATE NAME	DESCRIPTION
OUs and Domains - Group Policy Modeling	When applied to an OU or domain, allows the Trustee to perform Group Policy modeling for users and computers in that OU or domain.
OUs and Domains - Create and Link GPOs	When applied to a container (domain or OU), allows the Trustee to create and link: select a container and create a GPO that will automatically be linked to that container.
GPO Links - Create, Modify, Delete	When applied to a container, allows the Trustee to link existing GPOs to the container, to delete existing GPO links and to modify GPO link options such as No Override and Disabled.
GPOs - Change Status	Allows the Trustee to specify whether the user configuration settings or computer configuration settings in the GPO should be processed.
GPOs - Security Settings	Grants the trustee read/write access to the policy settings in the following categories: Account Policies, Local Policies, and Event Log.
GPOs - Restricted Groups	Grants the Trustee read/write access to the Restricted Groups policy settings.
GPOs - Administrative Templates	Grants the Trustee read/write access to the registry-based policy settings specified with Administrative Templates

TEMPLATE NAME	DESCRIPTION
GPOs - Scripts	Allows the Trustee to specify scripts that are to be run when the computer starts up or shuts down, or when the user logs on or logs off the computer.
GPOs - Folder Redirection	Grants the Trustee read/write access to the Folder Redirection policy settings.

Active Directory Security Management

The ActiveRoles Server MMC Interface makes it easy to examine and manage permission entries in Active Directory, by showing the access available to each user, along with the scope of their access. A centralized view of all permission entries for any given object helps with the analysis and administration of permissions in Active Directory. For each permission entry, the view displays a number of entry properties, including the permission description, origin, and security principal. From the main window, additional properties can be displayed and the native security editor can be accessed.

The centralized display of native security allows the administrator to quickly view permissions assigned to objects in Active Directory, and to determine whether the permission is inherited. The list of permission entries can be sorted by security principal name to determine who has access to the selected object. If a permission entry is inherited, ActiveRoles Server identifies the object from which the permission originates, so that the administrator can easily find and edit the permission entry for that object.

The ActiveRoles Server MMC Interface provides the capability to view the permissions for an object by simply clicking the object to display the permission entries in a centralized view. This makes it easier for the administrator to verify the permissions on security-sensitive objects, and to identify possible security problems.

Management of Native Security

ActiveRoles Server Access Templates can be used to specify permissions in Active Directory. Designed to support the role-based grouping of permissions, Access Templates provide an efficient mechanism for setting and maintaining access control, simplifying and enhancing the management of permissions in Active Directory.

To provide this capability, ActiveRoles Server gives the administrator the option to keep Active Directory native security updated with selected permissions specified using Access Templates. This option, referred to as **Permissions Propagation**, is intended to provision users and applications with native permissions to Active Directory. The normal operation of ActiveRoles Server does not rely on this option.

For ActiveRoles Server permission entries with the **Permissions Propagation** option set, ActiveRoles Server generates Active Directory native permission entries in accordance with the ActiveRoles Server permissions. Once set, the option ensures that every time ActiveRoles Server permission assignments or templates change, the associated native permission entries change accordingly.

ADSI Provider and Script Policy to Support Customization

ActiveRoles Server offers the facility to customize its off-the-shelf functionality using scripts and applications that interact with the Administration Service. It allows a high degree of customer modification to meet specific business and organizational needs. This gives customers greater flexibility when using the product, and enables them to build solutions that can easily be integrated with existing systems and data. The following list shows some of the ways in which the product can be customized:

- Using the ActiveRoles Server ADSI Provider, the existing proprietary applications or custom Web-based interfaces could communicate with ActiveRoles Server to perform administration and provisioning tasks on user accounts and groups.
- Using policy scripts, custom corporate rules could be enforced to regulate data format and administrative workflows.
- Using policy scripts, the data stored in a Human Resources database or ERP system could be incorporated into the administration and provision of user accounts.

ActiveRoles Server makes it possible for user-developed scripts and applications to manipulate directory objects through the Administration Service (*persistent objects*), and to take control of objects that are in the process of being created, modified, or deleted with ActiveRoles Server (*in-process objects*).

Having programmatic access to persistent and in-process objects makes it easy for developers to customize ActiveRoles Server in these two areas:

- Creating custom applications and user interfaces
- Enforcing corporate administrative policies by running custom scripts (*script policies*)

Custom Applications and User Interfaces

A custom application or user interface can be created to manipulate directory objects in ActiveRoles Server. ActiveRoles Server offers the developer an efficient means to communicate with the Administration Service—the ActiveRoles Server ADSI Provider. The ActiveRoles Server ADSI Provider enables custom applications and scripts to access directory objects using standard COM interfaces that conform to the Microsoft ADSI 2.5 specification.

Custom applications are executables that provide data to the Administration Service or retrieve and process data from the Administration Service. For example, an organization with a separate Human Resources database could develop and deploy a custom application that extracts personal information from the database, and then passes it to the Administration Service in order to facilitate user account provisioning.

Custom user interfaces are usually Web-based interfaces that distribute certain tasks to users. Custom user interfaces can also be used to streamline the workflow of network administrators and help-desk operators. For example, Web-based pages could be created so that help-desk operators only see the fields related to user properties that they can view and modify, according to the corporate standards.

Both custom applications and user interfaces rely on the ActiveRoles Server ADSI Provider to access the functionality of ActiveRoles Server.

Custom Script Policies

ActiveRoles Server provides the ability to implement administrative policies by running user-developed scripts (custom script policies). This makes it easy for policy scripts to manipulate both in-process and persistent object data in order to:

- Facilitate the provisioning of user accounts—populate user properties through external database integration and automate multi-step provisioning tasks.
- Maintain the integrity of directory content—prevent inconsistency of Active Directory data by enforcing update-sequence and data-format policies across the enterprise.
- Enforce business rules—maintain security design and capture administration expertise by integrating business rules into the administrative workflow.

Once configured, custom script policies are enforced without user interaction. ActiveRoles Server automatically handles the execution of policy scripts that supplement particular administrative operations and trigger additional administrative actions. For example, policy scripts can be used to:

- Perform a sophisticated validity check on input data
- Synchronously change information in multiple data sources, such as the Active Directory store, Microsoft Exchange server, and HR or ERP-system database
- Ensure that delegated administrators follow a prescribed administrative workflow
- Link multiple administrative tasks into one operator transaction

Dynamic Groups

ActiveRoles Server helps streamline group maintenance by defining group membership dynamically, with rule-based membership criteria. Dynamic group membership eliminates the need to manually update membership lists for security and distribution groups.

To automate the maintenance of group membership lists, ActiveRoles Server provides:

- Rule-based mechanism that automatically adds and removes objects to groups whenever object attributes change in Active Directory
- Flexible membership criteria that enable both query-based and static population of groups

The membership criteria fall into these categories:

- **Include Explicitly**—Ensures that specified objects are included in the membership list regardless of any changes made to the objects.
- **Include by Query**—Populates the membership list with objects that have certain properties. When an object is created, or when its properties are changed, ActiveRoles Server adds or removes it from the membership list depending on whether the object's properties match the search criteria.
- **Include Group Members**—Populates the membership list with members of specified selected groups. When an object is added or removed from the selected groups, ActiveRoles Server adds or removes that object from the membership list.
- **Exclude Explicitly**—Ensures that specified objects are not in the membership list regardless of any changes made to the objects.
- **Exclude by Query**—Ensures that objects with certain properties are not in the membership list. ActiveRoles Server automatically removes objects from the membership list depending on whether the objects' properties match the search criteria.
- **Exclude Group Members**—Ensures that members of specified groups are not in the membership list. When an object is added to any one of the selected groups, ActiveRoles Server automatically removes that object from the membership list.

These membership criteria are also applicable to Managed Units.

Web Interface—Simple to Use, Easy to Customize

The ActiveRoles Server Web Interface is a customizable, easy-to-use Web-based application that facilitates administration, while taking full advantage of ActiveRoles Server's security, workflow integration, and reporting benefits. To help distribute administrative tasks, the Web Interface offers the facility to configure multiple Web sites with individual sets of user interface elements. Each Web site can be customized to meet specific business and organizational needs.

Key features of the Web Interface include the following.

Role-Based Suite of Interfaces

Customized interfaces (Web sites) can be installed and configured for administrators, help desk operators, and end users. Administrators use an interface that supports a wide range of tasks, whereas help desk operators use a tailored, dedicated interface to expedite the resolution of trouble tickets. Network end users have access to a special interface for self-administration. Because multiple interfaces (Web sites) with different configurations can coexist on the network, there is no need to re-configure the Web Interface for particular roles.

Dynamic Configuration Based on Roles

The Web Interface dynamically adapts to the specific roles assigned to the users. A user can see only the commands, directory objects, and object properties to which the user's role provides administrative access. Objects and commands beyond the scope of the user are removed from the Web Interface, streamlining the execution of administrative tasks.

Point-and-Click Customization

It is straightforward to configure the user interface. Administrators can set up a suitable set of user interface elements without writing a single line of code. Administrators can add and remove commands or entire menus, assign tasks and forms to commands, modify forms used to perform tasks, and create new commands, tasks, and forms. All configuration settings are saved in a persistent storage so that the Web Interface users are always presented with the properly configured interfaces that suite their roles.

Instant Application of Administrative Policies

User input is efficiently supplemented and restricted based on administrative policies defined in ActiveRoles Server. The Web Interface displays property values generated in accordance with the policies, and prohibits the input of data that violates them. User input is checked against the policies before committing the operation request, and if a violation is detected, the user can immediately correct the input.

Fully Featured Management of Active Directory Objects and Computer Resources

The Web Interface supports all administrative tasks on Active Directory objects such as users, groups, and computers, and on computer resources such as services, printers, network shares, devices, system registry, and local users and groups. The Web Interface is suitable for all categories of user with administrative rights, from highly privileged administrators to Help Desk operators. With its advanced customization capabilities, the Web Interface serves as a complete administrative tool, providing suitable interfaces for any administrative role.

Support for Self-Administration

Provided they have the necessary ActiveRoles Server permissions, end users can carry out self-administrative tasks, such as modifying their personal data. Due to the reliable enforcement of business rules based directory entry in ActiveRoles Server, the Web Interface makes self-administration safe and secure, while at the same time providing increased service levels.

Support for Multiple Languages

The Web Interface allows users to select their preferred language. Changing the language affects all menus, commands, and forms associated with the Web Interface, as well as tool tips and help.

Different Interfaces for Different Roles

The Web Interface allows multiple Web sites to be installed with individual, customizable configurations. The following configuration templates are available out-of-the box:

- **Site for Administrators**—Supports a broad range of tasks, including the management of all directory objects and computer resources.
- **Site for Help Desk**—Handles typical tasks performed by Help Desk operators, such as enabling/disabling accounts, resetting passwords, and modifying select properties of users and groups.
- **Site for Self-Administration**—Allows users to manage their own accounts in Active Directory. Users can perform self-administration within the scope of the administrative authority delegated to them in the ActiveRoles Server environment.

Each Web site configuration template provides an individual set of commands installed by default. The Web site can be customized by adding or removing commands, and by modifying Web pages (forms) associated with commands.

Although the Web Interface dynamically adapts to roles assigned to users, the ability to tailor separate Web sites to individual roles gives increased flexibility to the customer. It helps streamline the workflow of directory administrators and help-desk personnel. Static configuration of interface elements ensures that Web Interface users have access to the specific commands and pages needed to perform their duties.

Role-Based Management of Computer Resources

ActiveRoles Server provides the capability to delegate administration of computer resources, such as network shares, services, and printers. Delegated administrators can use the ActiveRoles Server Web Interface to manage computer resources with a single, consolidated tool.

ActiveRoles Server, along with the Web Interface, enables delegation of administrative tasks on the following computer resources:

- **Network shares**—Create share, view/modify share properties, stop sharing
- **Services**—Start/stop service, view/modify service properties
- **Local groups**—Create/delete group, add/remove members, rename group, view/modify group properties
- **Local users**—Create/delete user, set user password, rename user, view/modify user properties

- **Logical printers**—Pause/resume/cancel printing, list documents being printed, view/modify printer properties
- **Documents being printed (print jobs)—** Pause/resume/cancel/restart document printing, view/modify document properties

The Web Interface also enables the management of the following computer resources:

- **Registry**—Create/delete and view/modify registry keys and values
- **Devices**—View/modify device properties, start/stop devices

Hardware and Software Requirements

ActiveRoles Server is comprised of the Administration Service and user interfaces, including the MMC interface and the Web interface. Reporting requires the installation of additional components. The tables below outline system requirements for installing and running the product.

The hardware and software requirements for the Administration Service include:

PLATFORM	450 MHz or higher Intel Pentium-compatible CPU.
MEMORY	512 MB recommended. The amount required depends on the total number of managed objects (approximately 0.5 Kbytes per object).
HARD DISK SPACE	100 MB or more of free disk space. The amount required depends on the size of the Administration Database.
OPERATING SYSTEM	Microsoft Windows 2000 with Service Pack 3 or later, Windows XP, or Windows Server 2003.
SQL SERVER	Microsoft SQL Server 2000 or Microsoft SQL Server 2000 Desktop Engine (MSDE) Service Pack 3 for Microsoft SQL Server 2000 strongly recommended.

The hardware and software requirements for user interfaces include:

PLATFORM	450 MHz or higher Intel Pentium-compatible CPU.
MEMORY	256 MB recommended. The amount required depends on the number of objects being administered.
HARD DISK SPACE	The MMC interface requires about 40 MB.

OPERATING SYSTEM	Microsoft Windows 2000 or later.
INTERNET SERVICES	Microsoft Internet Information Server (IIS) 5.0 or later must be installed on the computer running the Web Interface.
WEB BROWSER	Microsoft Internet Explorer version 5.0 or later.

The hardware and software requirements for reporting components are outlined in the Reporting Console documentation that comes with ActiveRoles Server.

Licensing Model

The ActiveRoles Server licensing model is based on the number of enabled user accounts in the managed domains. The total number of enabled user accounts in all managed domains cannot exceed the licensed amount.

The number of licenses required is equal to the total number of user accounts within all managed domains. ActiveRoles Server allows you to explicitly define a list of managed domains. This helps prevent the total number of user accounts from exceeding the licensed amount.

The following items are not limited by the licensing agreement:

- The number of delegated administrators (Trustees)
- The number of computers running the ActiveRoles Server user interfaces
- The number of Administration Services—in a large enterprise, Administration Service can be installed on multiple computers for enhanced performance and fault tolerance

Once started, the Administration Service reports the following license information to the event log on the computer running the ActiveRoles Administration Service:

- The number of licenses purchased by the organization.
- The number of user accounts retrieved by the Administration Service
- The license expiry date

If the number of users is greater than the licensed amount, the Administration Service continues to process requests, but the number of user accounts it can retrieve is limited to the licensed number. When registering a managed domain, one consideration should be made—the Administration Service cannot manage an additional domain, if the number of user accounts in that domain exceeds the number of free licenses, that is, the number of licenses not already allocated to other managed domains.

Examples of Use

ActiveRoles Server can be configured to provide a wide range of directory management solutions, allowing organizations to create more secure, productive, and manageable Active Directory and Microsoft Exchange environments. This section highlights how ActiveRoles Server helps to address the challenges faced by enterprises today.

Distributing Administration

Suppose a large company wants to introduce distributed administration, but wants to avoid the large costs involved in training their Help Desk and business units to correctly use complex administrative tools. In this situation, there is the need for an easy-to-use tool, to control what actions the Help Desk and business units can perform, and to enforce company policies and procedures.

Solution

ActiveRoles Server allows organizations to create Managed Units and to designate Trustees over those Managed Units. Trustees only see the objects to which they have access. They are given only the rights they need for the objects within these Managed Units, down to individual properties. Unlike native Active Directory organizational units, Managed Units provide virtual boundaries that span across domains and forests, offering more flexible delegation capabilities.

Delegating limited control over Managed Units efficiently eliminates the need for high-level administrative user ID's, allowing organizations to securely distribute administrative authority to local management. To improve network security and make distributed administration safe, ActiveRoles Server defines and enforces customizable administrative polices.

ActiveRoles Server allows organizations to safely implement administration for business units. If a company has a number of different business units, each of equal importance and each located in a separate office, a single network administrator could support all of the sites. ActiveRoles Server allows the company to create a single Managed Unit, giving an administrator control over users and resources that span multiple domains.

Integrating with Other Systems to Simplify Corporate Provisioning

Suppose a company wants to integrate its HR system, administration, and physical security to provide a workflow that reduces repetitive data. Normally, the HR team creates a user profile, the IT team also creates a user profile in Windows and Exchange, and the security team activates an access card for the new employee. The three teams do not synchronize with each another and instead duplicate their work. This results in increased administration costs and introduces security issues. For example, some individuals may no longer work for the company but may still have valid user ID’s and access cards. In this scenario, there is a need to integrate the company’s HR system and other systems, and to automate the execution of user provisioning tasks.

Solution

With ActiveRoles Server, a suitable property set can be established to include data from network data sources other than Active Directory. For instance, a property set might be configured to retrieve a user’s personal information from an HR database. When the user account is created, this data could then be passed to Active Directory and Microsoft Exchange. If these property values change, an update could be made to both Active Directory and to the HR system.

ActiveRoles Server also provides the ability to set up administrative policies that reduce the amount of input required to carry out a task. For example, when a user moves to a different location, ActiveRoles Server could automatically update the user's profile in the HR system, based only on the change to the user's site code or department in Active Directory. Additionally, when a user joins or leaves the company, their access card could automatically be enabled or disabled.

Managing a Multi-Forest Active Directory Design

Suppose a host company has client customers who need to place domain controllers on their premises. In Active Directory, every domain controller holds a writable copy of the schema and configuration of the entire forest. Anyone with administrative or backup/restore rights on any domain controller, or physical access to any domain controller, could potentially disrupt the entire forest. For instance, they could attempt to circumvent Windows security, or they could edit the Active Directory database, and the changes would be propagated to all domains in the forest. To avoid such an incident, the company needs to create a separate forest for each client who requires domain controllers on their premises. Otherwise, the actions of one malicious user could affect directory service delivery for other clients in the same forest.

Having multiple forests increases the complexity of the Active Directory structure. This in turn leads to increased administration, as each forest needs separate directory service administration. In this case, there is a need for an administrative system that enables the cross-forest management of Active Directory.

Solution

ActiveRoles Server provides a unified management structure that can extend across multiple Active Directory forests. The ActiveRoles Server user interface provides a single interface for the management of Active Directory domains that belong to different forests. It offers administrative views (Managed Units) that can hold objects from multiple forests, thereby enabling the unified application of corporate rules and roles across forest boundaries.

With its ability to safely delegate administration in multi-forest environments, ActiveRoles Server provides the necessary level of control for the host company's customers, while enabling the company to implement role-based security, and restrict the customers' administrative actions based on corporate policies.

For security reasons, it may be unacceptable to have an administrative tool with the same level of rights as a domain administrator. This is because administrative access to an entire domain in a forest may be used to gain administrative access to the whole forest, via the elevation of privileges attack. ActiveRoles Server can operate in a multi-forest environment within a precisely defined scope of access to domains, with no special requirement to have administrative access to entire domains or security-sensitive containers. This addresses the need for a product that provides advanced administrative capabilities, while effectively preventing the elevation of privileges.

Simplifying Active Directory Structure

Suppose a company wants to design an Active Directory structure based on physical location. As a rule, the administration/IT department, business units, and Exchange team would each prefer to have a different structure. As a result, they agree to a compromise that doesn't fully satisfy their requirements. Clearly, there is a need to simplify the Active Directory structural requirements.

Solution

In ActiveRoles Server, Managed Units allow organizations to achieve acceptable security boundaries without setting up extra domains or Organizational Units. This significantly simplifies the Active Directory structure and reduces security risks.

By using Managed Units for delegation purposes, ActiveRoles Server creates a rule-based overlay of Active Directory for administration. This simplifies the process of choosing an Active Directory structure. Different administrative tasks often require different OU structures. For instance, an OU structure designed purely for the delegation of administration differs from an OU structure shaped purely for Group Policy. It becomes much easier to design an Active Directory structure by using Managed Units to handle delegation issues.

Handling Organizational Changes

Consider a company in the process of re-organization. Multiple departments are changing names, merging, or separating from one another. Such reorganization involves an increase in administrative, security, and business liabilities, as well as the high cost of manually updating data. This situation demands a means to automatically update and move the data.

Solution

ActiveRoles Server provides the ability to define administrative policies that make organizational changes easier to handle. By using Managed Units, rule-based overlays of the actual data in Active Directory can be set up for both the current and planned organizational structures. Administrative policies can be specified so that when data moves from one Managed Unit to another, policy definitions will automatically be applied, based on the change. This will update properties, such as the user's manager, department, group memberships, and OU memberships.

As another example, consider a user who changes departments. Depending on the department to which the user moves, ActiveRoles Server could automatically move the user's data, change the user's group memberships, and specify to whom the user reports.

Account Provisioning in ASP-Hosted Environments

Suppose a company wants to become an Application Service Provider (ASP), with the intention of creating a package to provide services based on Active Directory and Microsoft Exchange. The company relies on the Active Directory infrastructure as a basis for their service offerings.

Configuration of Active Directory in an ASP-hosted environment involves setting security and partitioning the directory, so that any customer connected to the host infrastructure has proper access to its directory resources. It is paramount to have a framework that facilitates the creation of new customers and the assignment of appropriate access rights. In this scenario, there is a need for a robust provisioning system that maintains customer sign-up, configuration, and user management for hosted services, with minimal administrative effort.

Solution

ActiveRoles Server offers a reliable solution to simplify and safely distribute account management and provisioning in an Application Service Provider (ASP) environment. It addresses the need to create and manage a large number of user accounts originating from a wide range of customers, and to ensure that each customer can only access their own resources. By implementing an administrative model based on business rules, ActiveRoles Server allows domain-level administrators to easily establish and maintain very tight security, while facilitating the provisioning of new customers with the appropriate access rights.

ActiveRoles Server has the ability to safely delegate routine user-management tasks to designated users in a hosted organization. It therefore provides the necessary level of control for the ASP customers and helps the ASP to reduce management costs. By incorporating policy enforcement and role-based security, ActiveRoles Server allows an ASP to restrict its customer administrative actions according to the corporate policies defined by the ASP. In addition, it allows the ASP to change the policy, ensuring that new policy settings are automatically propagated and enforced without additional development.

ActiveRoles Server makes it simpler for an ASP to delegate authority to administrative and support groups within the customers' organizations, while enhancing the overall security. The Web interface can serve as a customer-driven provisioning tool that allows the customers' administrators to manage users, groups, and mailboxes. ActiveRoles Server ensures that all actions performed by a Web interface user conform to the ASP corporate security policies.

Summary

ActiveRoles Server delivers a reliable, policy-based administration and provisioning solution, allowing enterprises to fully benefit from Active Directory and Microsoft Exchange deployment.

One of the most valuable features of the product is the ability to automate provisioning tasks on directory objects in compliance with corporate administrative policies in corporate Active Directory and Exchange environments.

ActiveRoles Server provides consistent enforcement of corporate policies, a role-based administrative model, and flexible, rule-based administrative views, creating a reliable and secure environment for distributed administration and account provisioning.